MICROSOFT WINDOWS NT™

网络安全、审查与控制

Microsoft WINDOWS NT SERVER 安全性专辑

希望 学苑出版社

Microsoft®

微机新软件系列丛书

网络安全、审查与控制

Windows NT Server 安全性专辑

刘 霞 丁红兵 主编

学苑出版社

Microsoft®

(京)新登字 151 号

内 容 提 要

本书介绍了网络的安全、授权和管理策略，以及 Windows NT 安全、审查和控制，是系统管理员、安全员及客户机/服务器用户的必备参考书。

欲购本书的用户，请直接与北京海淀 8721 信箱书刊部联系，电话：2562329，邮政编码：100080。

版 权 声 明

微机新软件系列丛书

网络安全、审查与控制

Windows NT Server 安全性专辑

主　　编：刘　鹰　丁红兵

责任编辑：甄国宪

出版发行：学苑出版社　　**邮政编码**：100036

社　　址：北京市海淀区万寿路西街 11 号

印　　刷：北京市地质矿产局印刷厂印刷

开　　本：850×1168　1/16

印　　张：9.125　　**字　数**：210 千字

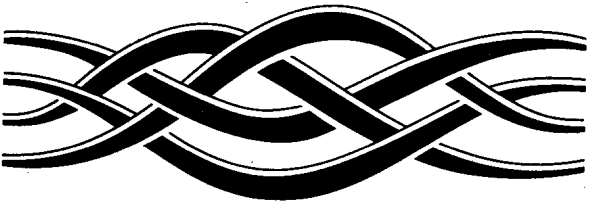
印　　数：1～5000 册

版　　次：1994 年 10 月北京第 1 版第 1 次

ISBN7－5077－0976－0/TP・35

本册定价：19.00 元

学苑版图书印、装错误可随时退换



巨大的效益
——使用NT的结果

Microsoft

主　　编：刘　霞　丁红兵
编　　委：张彤川　李　浩　陈　平
　　罗　川　王静茹　吴　杰

出版：微软公司北京办事处
地址：北京新世纪饭店写字楼5层551室
邮编：100046
电话：8492148－50
传真：8492151

介　绍

Windows NT 3.5 安全、审查、控制指南用于帮助系统管理员、安全专家、审查员和用户，理解 Microsoft Windows NT Server 3.5 操作系统控制、安全、审查的执行过程。通过提供 Windows NT Server 企业规划方法，为系统审查员、安全专家和最终用户提供了企业级安全和控制标准。它指导用户通过使用 Windows NT 的一系列复杂工具来建立企业级可信赖的环境。本书组成结构如下：

章节	主要对象	次要对象
1	管理员	所有 EDP 审查员、系统安全管理员、客户机－服务器管理员、开发者
2	安全管理员、客户机－服务器管理员、EDP 审查者	管理员、开发者
3	EDP 审查者	客户机－服务器管理员、系统安全管理员、系统管理员

鸣谢：

本书的创作是真诚合作的结晶。曾经得到了许多人的支持和帮助。特别感谢曾帮助我确定题目的 Microsoft 公司的 Bill Anderson 先生和帮助本书出版的 Microsoft 出版社的 Jim Brown 先生。另外还要感谢给我许多宝贵经验的 Citibank 安全协作部门副经理 David B. Morrison 先生，以及 AL Decker，Partner，Coopers 和 Lybrand 等。还要感谢 IIA(Institute of Internal Auditors)技术部经理 Charles H. Le Grand，感谢他个人给予我的支持和帮助。同样也要感谢 Alan S. Oliphant，Standard Life Assurance Co. 和 Joseph Burke，Metropolitan Life Insurance Co. 和 Fazal Khan，Kevin Phaup，和 Frank Artale，感谢他们给予我许多背景资料和技术文献。

本书作者曾经工作于许多公司、地区，积累了关于此论题大量丰富的写作经验。特别提及要感谢 Shane Gonzales，Sue Wyble，Gwen Gray，Sharon Carroll，Dyana Nguyen，Karin Carter，Diana Rain，和 Kerry Lehto 等 Microsoft 公司献身本专题的开发人员。非常感谢他们给予了我们讨论本专题的机会。

前　言

IIA (The Institute of Internal Auditors) 非常愉快的加入与 Microsoft, Citibank, N. A., 和 Coopers&Lybrand 的合作行列，来为 Windows NT 环境设计执行安全审查的策略指南。IIA 组的审查者和安全专家花费了大量的时间来写作这个专题。

尽管网内连接工作站，服务器和网际互连的论题相对于传统的信息系统还比较年轻，但这个问题的讨论和解决方法已经多种多样了。迁移重要的商业应用程序到企业网络中去会导致新层次的用户安全问题，而以前的系统是通过数据中心解决的。现在企业网络需要提供内部控制、安全和审查的能力。

专业审查系统需要将内部控制作为管理的对象，并详述适合控制任务的结构框架。National Commission on Fraudulent Financial Reporting (Treadway Commission, 1987) 的报告详细阐述了管理、指导范围、审查方式和法律规定等问题。这个报告就加强政府和财政系统的可靠性提出了许多建议。The Committee of Sponsoring Organizations of the Treadway Commission (COSO) 详尽考察了这个报告并于 1992 年发布了定义内部控制的 COSO 报告。以及"集成网络内部控制"问题的论述。IIA 是 COSO 的成员之一，在改进管理工作和内部控制方面作出了许多努力。

IIA 研究机构于 1991 公布了系统审查控制 (SAC) 报告，1994 年第三季度又公布了改进的报告。

SAC 这个关键的报告成果主要为加强系统管理员、设计者、开发者、用户、和审查者提供保证安全、审查系统环境设置的能力。SAC 已经成为定义、考察所有计算机系统风险和控制问题的有力参考。

IIA 同样提供了"内部审查的专业标准"。

本书可以用来作为 Windows NT Server 环境的安全运行和审查的基本知识和操作指南。IIA 并不与任何开发商就控制和安全方面签署条例，但愿意参与产品安全、控制和审查等方面的讨论。IIA 非常愿意与工业、技术领域的开发团体合作，在他们发布产品前共同研究产品控制和审查等方面的问题。

这是 IIA 关于 International Advanced Technology Committee 的第二个成果，也是专业审查机构与工业合作改进技术的成功例子。为管理员、开发者、用户和审查员提供专业知识是非常重要的。我们感谢 Microsoft 在这个方面的先锋作用，使我们有机会检视我们提出的报告。他们对我们报告有改进的接受，增强了控制、审查原则的质量。

Charles H. Le Grand

Director of Technology, Institute of Internal Auditors

目　录

第一章
安全，审查和控制策略

在迈入信息社会的今天，产业、政府和个人越来越依赖于他们的信息资源，并且投入了数以亿计的经费来保证数据处理、数据转换和存储的安全可靠性。于是安全、管理和审查过程成为设计和管理信息系统的一个重要组成部分。

二十五年前，IBM、DEC、和其他计算机公司在保证他们的主机系统安全性方面曾做出很大的努力。政府和学术界联合起来共同决定怎样才能保证主机系统的安全性。当时有一句尽人皆知的话："五年内我们将会有安全的操作系统…"。

今天，计算机公司已转向客户机－服务器方式，崭新的技术大量涌现。Client－Server 方式使我们重新考虑安全性。既要满足多种不同环境的协同运算。又要建立一个安全可控的 Client—Server 环境，这成为一个复杂的问题。政府条文、国际数据控制流规定、安全保密要求、通讯连接等附加给计算机公司大量新的问题和要求。

新操作环境负担了繁重的审查和安全管理工作。管理员、审查员和安全专家面临管理大量设备和服务程序的任务。一个操作系统本身要具备在 Client－Server 环境下提供安全和审查的能力。Microsoft Windows NT Server 正是基于这种要求设计的。本书将主要介绍 Windows NT 操作系统的审查管理方法。

Windows NT 和局域网安全

审查必须定义和检查包含现今网络平台的各种组件：操作系统、国内和国际通讯设备、操作和运转过程、硬件和软件选型策略。审查者需要制定一种有序审查和分析公司或企业网络的方法。审查者要将数据处理过程加以控制监测并且保证控制过程始终处于自我诊断的状态。今天，像 Microsoft 的 Windows NT 这样强大的新操作系统能够满足企业级的要求。Microsoft 将安全和审查特色集成到 Windows NT 系列产品中。

Windows NT 是真正的 32 位抢先式多任务操作系统，更重要的是 Windows NT 设计中将安全和审查作为操作系统的组成部分。Windows NT 通过美国国防部 C2 级标准认可。相容性是 NT 设计的另一个目标，这样就保证系统能跨越大量符合工业标准的 CISC 和 RISC 平台。

Microsoft Windows NT Server 提供了强大的用户和资源安全保护功能。Windows NT 的服务程序结合明确清晰的安全控制需求，允许用户完成下面的工作：

- 特殊的存取控制

· 安全标准化
· 审查认证－实时检测
· 安全相容性
· 安全管理－集中化和分布式

系统管理员在 Windows NT 平台执行工作时要考虑：

· 在混合环境中执行 Client－Server 方式时，系统管理员会面临跨平台用户的认证管理问题。管理员必须清楚跨平台时会遇到的安全相容等技术和协议标准。
· 系统管理员一定要制定网络安全和审查的标准，当需要升级和改进系统时要保证原有的规则不会被改变。
· Windows NT 不能进行无安全性的安装。原因在于开放网络环境缺省情况下要求系统为封闭状态，来允许执行程序更好的理解和检测安全子系统。
· Windows NT 制定了用户级别安全措施，因而要仔细考虑用户具有的权限和用户所能使用的资源。

安全目的

信息技术(IT)目前已成为企业基础的一个组成部分。离开(IT)企业在高科技的今天将失去竞争活力。

信息数据的安全要求非常严格。当企业信息系统应用 Cient－Server 技术逐步转化成为分布式系统时，信息需要经常往返于复杂的通讯网络。这些通讯网络的连接也必须被考虑成为计算环境负荷的一种。因此在任何安全系统都需要将网络登录和远程连接集成为其中的一个组成部分。依靠主机系统的安全技术已经不能保证网络数据的安全。传统的基于主机的安全系统必须延伸到局域网(LAN)和广域网(WAN)，从而对在节点间流动的数据信息进行保护。网络连通是安全的基础，然后所有的网络节点按预先定义的标准配置，从而达到最低的网络安全要求－信息共享。

为保证网络的最低安全要求，必须提出企业级别的安全标准，来物理和逻辑控制软件和硬件。没有统一的标准，在组织内部会有许多不便，并引发出许多问题。企业的信息安全策略应该包含统一标准和如何使用主机、LANs、工作站、PCs 和网络中的其他组件。这种策略指南要详尽指出影响信息安全的主要问题和解决方法如：

· 保密性－防止非法侵入未审查的敏感信息
· 完整性－对信息数据的准确性和完整性自我保护能力
· 允许性－保证信息和重要的资源在需要时能被用户所使用

对网络信息资源的划分应该制定一个不变的的安全管理方案。对网络资源的外部存取也需要有特定的方法，为保证最低的安全性要求，需要为主机和应用程序指定存取控制、登录认证、权限和资源配置等方式。

安全揭密

执行和维护多平台计算环境的安全系统是大家正在考虑的问题。许多公司的网络具有多工作地点、多工作平台、多个应用者，并连接到外部的公共信息网上。这种需求提高了企业网络最低程度的要求－网络信息共享。信息能够传输到网络的各个节点，例如：另外的主机、网络设备、个人机、工作站和文件服务器。因为所有的设备均位于网络中，一旦其中的一个组件得到授权允许，它就可以作为进入网络的一个入口。所以从安全的角度来看，所有的主机、服务器、工作站、网络节点和组件都非常重要。

计算机存取控制，无论主机系统、小型机、工作站、或 PC 机都可以分为两种方式：

- 本地机或主机－终端存取方式
- 网络或远程存取方式

本地机，或主机－终端存取方式能很好控制因为这种技术已经非常成熟。“信赖计算机系统”(DoD85)一书，详细罗列了存取控制的标准。制造商可以按他们的要求选择书中的任一标准。

相反，网络或远程存取标准并不明确。像拨号、网络路由、网络协议或服务程序过滤、网络登录和认证、文件传输、电子邮件和 Internet 网的连接也只是目前讨论到的一些安全管理问题。这些问题已经有许多厂家的产品，每种产品不仅遵循兼容性、互连性、和扩充性，还有许多自己的特色。

通常，信息的使用配置是并不考虑安全含义的。例如，选择 TCP/IP 作为网络协议意味一个网络安全管理员在决定协议之前作出其他决定。这些决定包含网络允许的服务程序(FTP，TELNET 等)，是否加入 Internet 网，哪一个节点可以看成值得信赖(允许无 Password 登录)，或者是否使用网络安全设备(例如应用程序 Gateway 或 Firewall)。当内部联网成为商业需要时，网络安全方案将显示出它优越于主机存取方式的特色。

因为网络不同部分的安全任务遵循不同的组织形式、操作规则和规程，所以会有不同的标准，这就造成横向不一致。同样也会有纵向的不一致。当信息技术过渡到 Client－Server 方式下时安全责任转向前台用户。前台用户还没有足够的安全任务的准备。事实上当计算任务大量分散到前台时，就会造成缺乏对新任务正式、一致的策略，这种操作方式使得网络极易受到损害，包括，非法使用、数据损坏、丢失、破坏、和修改。如何解决这个问题是本书的焦点。

一个全面的安全策略不仅应该包含对大型机系统、中型机系统和工作站足够的安全考虑，还要包含对局域网(LANs)、Client－Server 结构、网络协议、个人机、网络资源和设备等的安全考虑。安全策略还应考虑网络互连的问题。

信息安全性

信息的安全性是一个涉及面非常广的题目。它不是简单的物理安全－锁住一台计算机并把它放到一间锁住的房间内。它也不仅仅是要求登录 ID 和相应的口令，对

文件授予权限防止非法存取和意外损坏，网络数据传输中的保密数据，或防止电磁干扰等问题。有效的信息安全系统要求物理上、管理上和操作策略上都有很强的安全和审查特色。并且非常有助于减少网络风险和泄密。信息安全系统会防止恶意入侵和意外存取、损坏、或数据丢失。

安全系统仍然需要由人来计划和管理，即使最好、最值得信赖的系统例如 Windows NT，安全性也不能完全由计算机系统独立承担保障的任务。系统管理员和最终用户都要执行、监测、和遵守安全规定。

控制方法

为了加入和防止 Client－Server 系统中可能发生的问题，对全盘一定要有预先考虑的计划。在安装系统前，要考虑下面的一些问题，特殊的问题将在后面的附录中介绍。

Technical Area	Concern
设计策略	在安装运行 Windows NT 之前理解本企业的组成结构和数据流向，为了使企业网络提供最高的可靠性，系统必须运行于可控的环境。好的设计是完成达到目的的关键，这就要求尽可能早参与审查和安全的设计。
Client－Server 安全性	Client－Server 操作系统应该提供对系统组成部分物理和逻辑上的安全。新系统至少应该提供同层次上安全、审查前台、后台、应用程序、用户和界面等的开发指导。
加密和认证	Windows NT 提供加密存储和加密传输但对于通讯安全来说还不够。
审查和管理	使用有效的安全控制工具。对新增的用户存取控制、管理和操作将成为一个复杂、费力的工作。为保证一个有效的安全系统，需要各个层次的人为设计和审查，集中于要求严格的、敏感的系统、连续的工作流程和人员培训。
网络分析	衡量网络的效率、可靠及性能。必须了解使用网络的企业目标和企业运转过程，只有这样才能提供对企业的最有效的支持。

Client－Server 环境中的审查问题

Client－Server 计算环境通过提高信息的实用性使商业团体更充分地利用信息资源。现在信息可以在用户的桌面电脑、或掌上型电脑中，抛开时间、地点等限制灵活的利用。

Client－Server 环境除了**节省资金**外，还能给开发和执行应用程序带来好处。例如，系统开发可以在工作站上进行，工作站会提供大量的服务程序包括：图形界面(GUI)、图像、视频技术和**多媒体**。用户现在可以方便有效地执行写作、数据分析、提炼模型等工作。而无需考虑所使用的数据的来源和存储位置，用户对数据的访问可以是实时的、一致的，这一过程对用户来说又是透明的。应用程序的运行和数据访问可以分散到客户机和服务器上，以达到最优的程序设计逻辑、数据检索和网络吞吐。

基于安全性能差的微型机和局域网上的 Client－Server 技术给安全审查者提出了新的问题。在这样的系统中许多数据中心的安全和信赖关系在最初并没有建立。这种新技术的基础还要有多种应用程序的支持，不仅包括第三方厂家的应用程序；字处理、电子表格、数据库、图形工具包，还包括利用操作系统原码写成的系统配置文件。

在 Client－Server 结构下，系统被逻辑分为几个部分，客户机、网络、服务器，从安全和审查的观点来看这几部分要么单独考虑，要么与系统集成考虑。当 GUI、应用程序和 DBMS 位于服务器或主机上时，控制是集中的并与主机的安全度相一致。但当应用程序和 DBMS 驻留于多个服务器和工作站、PC 机上时，审查者必须将客户机和网络中会遇到的问题也考虑在内。

当数据分散于 Client 和 Server，就会面临下面一些问题：

- 责任，数据的责任不明确。谁是数据的所有者？谁是数据的应用者？对数据操作任务是否有足够的分离。
- 用户培训和安全认识：当程序和数据文件从主机、服务器流向客户机和用户时，需要使用者有足够的经验和能力来完成此项工作。产生的数据位于个人机或用户桌面上的工作站，用户必须负担起自己管理系统安全和系统备份的工作。大多数企业中，在这一方面用户还没有得到此足够的培训，甚至他们根本不想负担这份责任。
- 物理安全：因为个人机是放在用户的桌面上而非安全的数据中心，非法物理侵入问题就会发生。
- 开发和验证分离：如果系统或应用程序开发是在一个特殊的工作站上进行的，并且开发后的一部分系统仍存在于这里，那么在这里分离开发和验证环境就会变得更困难，需要审查。

因为 Client－Server 方式已成为我们信息技术的基本组成部分，这些问题必须要得到很好的解决。本章的后续内容将介绍企业如何建立一个具备 Client－Server 结构的安全的系统，以及这个问题在 Windows NT 中是如何得到解决的。

整体安全控制结构

安全系统的基础取决于它的整体安全结构的定义、执行、和监控。
企业的安全控制结构应该和它对信息的要求以及它所能承担的商业风险相一致。当商业需求改变时，商业风险也随之改变。所以控制结构是一个动态结构，定义控制结构的信息安全策略，也是一份活的论述，需要定期的考察和更新。
通常建立一个安全控制过程有下面几个部骤：
1. 论述、决定策略和过程。列出系统信息资源在组织上的标准，以及如何执行。
2. 执行过程和规定。进行功能明确的程序开发，用户培训。将安全管理手段以工具形式供用户使用。
3. 监控原则。监控是安全控制过程的一部分，能更有效的提高信息的安全程度，会提供定期、准确、相关的安全信息报告。
主要的安全控制结构如下。

安全策略和安全处理过程

一个网络系统应该收集和保存可以用来检测和分析违反系统安全策略的信息。为了使审查有意义，每次安装都要经过安全策略和安全处理过程的考虑。这可以看成为 Client—Server 模式下一条最基本的规定。对系统安全的改变和任何企图或实际对系统的存取控制的改变都可以看成违反安全规定的操作。

安全策略

整体安全框架包含一些主要的问题：
- 安全策略的范围和目标
- 企业信息资源的描述
- 从使用方法上对信息划分
- 使用者的责任
- 管理的责任
- 操作检测应考虑的问题

提出安全策略用来作为系统的标准、处理过程和行动的指南。这些论证要求可靠，供审查者使用作为高级管理和总体设计的标准。特定的用户指南和操作标准可以是仅与单独的用户相关，可靠性要求低的阐述。